①

Japanese Patent Laid-open Publication No.: 2001-326692 A
Publication date : November 22, 2001
Applicant : HITACHI Ltd.
Title : Interconnecting device and network system using the same

[0017]
One of the lines is used as an administration line 140 for exchanging various setting information among the interconnecting devices, and the remaining lines are used as lines for data 130.

[0028] The administration-information transmitting and receiving unit 350 obtains setting of the interconnecting device from the conversion-table administration unit 320 to construct a packet based on a protocol for exchanging the setting information between the interconnecting devices, and passes the packet to the external line communicating unit 370. The administration-information transmitting and receiving unit 350 receives the packet based on the setting exchange protocol between the interconnecting devices from the external line communicating unit 370 and interprets it, and passes the setting information to the conversion-table administration unit 320. In some cases, the administration-information transmitting and receiving unit 350 further constructs a return packet of the received packet, and passes it to the external line communicating unit 370.

[0031] The conversion table 325 is stored with protocol conversion information of each VPN-ID in a table format, as

shown in Fig. 4. Each conversion information includes: a VPN-ID 410; a partner VPN-ID 420; a connection netmask 430; a router address 440; a partner router address 450; an I/F identifier 460; a sequence number 470; and a flag 480.

[0032] The VPN-ID 410 is a number for uniquely identifying each VPN in a service provider to which the interconnecting device belongs, and the partner VPN-ID 420 is the VPN-ID within a service provider of the connecting partner. A VPN represented by the VPN-ID 410 and a VPN represented by the partner VPN-ID 420 are connected to each other. The connection netmask 430 is a netmask of an IP address assigned to a network between border routers of the both in the VPN-ID, and the router address 440 is an IP address of a border router in the network. The partner router address 450 is an IP address of a border router on the service provider side of a partner in the network. The I/F identifier 460 is an identifier of an interface used at the time of transmitting and receiving with an interconnecting device of the partner in the VPN-ID.

Firstly, the network administrator inputs the VPN-ID, the partner VPN-ID, the connection netmask, and the router address of the border router 120-A, and the I/F identifier of the interconnecting device 110-A, subject to conversion, into the interconnecting device 110-A (sequence 500).

[0036] (2) The interconnecting device 110-A temporarily registers the inputted information into the conversion table 325, setting the flag to the "waiting for temporary registration response". Subsequently, the interconnecting device 110-A transmits a VPN registration message including these pieces of information through the administration line to the interconnecting device B (sequence 510).

[0037] (3) The interconnecting device 110-B that receives the message temporarily registers the received transmission-side VPN-ID, receiving-side VPN-ID, connection netmask, transmission-side router address into the conversion table of its own, setting the flag to the "waiting for registration authorization".

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－326692
（P2001－326692A）
(43)公開日　平成13年11月22日(2001.11.22)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード(参考)
Ｈ０４Ｌ 12/66		Ｈ０４Ｌ 11/20	Ｂ	５Ｋ０３０
12/46		11/00	３１０Ｃ	５Ｋ０３３
12/28		11/20	１０２Ｄ	
12/56				

審査請求　未請求　請求項の数６　ＯＬ　（全 25 頁）

(21)出願番号　特願2000－143779(P2000－143779)

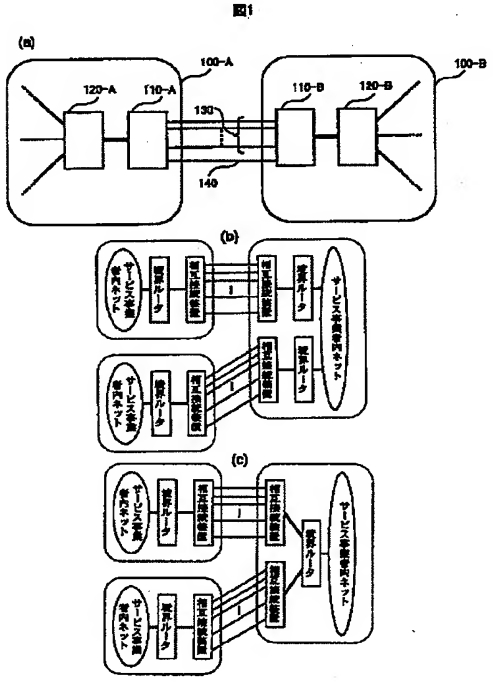
(22)出願日　平成12年５月16日(2000.5.16)

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　柘植　宗俊
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　川井　恵理
神奈川県秦野市堀山下１番地　株式会社日立製作所エンタープライズサーバ事業部内
(74)代理人　100078134
弁理士　武　顕次郎

Ｆターム(参考)　5K030 GA11 HA08 HC13 HD03 HD09
JA11 KA05 LD20 MC08
5K033 AA04 AA09 CB09 CC01 DB19

(54)【発明の名称】　相互接続装置及びこれを用いたネットワークシステム

(57)【要約】
【課題】　互いに異なる方式又は識別番号で複数の仮想プライベートネットワーク（ＶＰＮ）を管理している複数のネットワーク接続サービス事業者の間でＶＰＮ単位に相互接続する相互接続装置及び通信ネットワークシステム。
【解決手段】　各サービス事業者に、ＶＰＮの識別番号を含む内部ネットワーク用データパケットを送受信する内部ネットワークと、ＶＰＮの識別番号を含まないデータパケットを送受信し識別番号毎に異なる回線を持つ外部通信回線１３０との間で相互にデータパケットを変換する相互接続装置１１０を設ける。相互接続装置同士は、さらに別の管理用通信回線１４０によって接続され、互いのＶＰＮの変換情報を交換する。



1

【特許請求の範囲】

【請求項１】　特定のユーザに対して仮想的な専用通信路を提供する複数のネットワーク接続サービス事業者のネットワーク同士を相互接続するために、各ネットワーク接続サービス事業者のネットワーク毎に設置される相互接続装置において、前記特定のユーザを識別するために用いられる識別番号が付与されたデータパケットを第１のネットワークインタフェースから受信し、受信したデータパケットを前記識別番号を取り除いたデータパケットに変換し、変換したデータパケットを、相手側ネットワーク接続事業者との接続を行う前記識別番号毎に割り当てられた第２のネットワークインタフェースへ送信する手段と、前記識別番号のないデータパケットを前記第２のネットワークインタフェースから受信し、第２のネットワークインタフェース毎に割り当てられた前記識別番号を受信したデータパケットに付加し、第１のネットワークインタフェースへ送信する手段と、前記識別番号から対応する第２のネットワークインタフェースを導き出し、第２のネットワークインタフェースから対応する前記識別番号を導き出す前記識別番号と第２のネットワークインタフェースとの対応関係を保持する手段と、他のネットワーク接続サービス事業者のネットワークに設置された相互接続装置との間で通信を行って、前記識別番号と第２のインタフェースとの対応関係を交換する手段とを備えることを特徴とする相互接続装置。

【請求項２】　管理者が入出力装置を通して、あるいは、管理者が操作する装置との間で通信を行って、前記識別番号と第２のネットワークインタフェースとの対応関係を追加または削除する手段とを備えたことを特徴とする請求項１記載の相互接続装置。

【請求項３】　管理者が入出力装置を通して、あるいは、管理者が操作する装置との間で通信を行って、他のネットワーク接続サービス事業者のネットワークに設置された相互接続装置から受信した前記識別番号と第２のネットワークインタフェースとの対応関係に関する情報を確認し、これを設定することを承認する手段を備えたことを特徴とする請求項２記載の相互接続装置。

【請求項４】　前記識別番号付きデータパケットを送受信する第１のネットワークインタフェースに接続された装置に対して、前記識別番号に対応した通信に必要な情報を通知する手段を備えたことを特徴とする請求項１、２または３記載の相互接続装置。

【請求項５】　複数の通信ネットワーク相互間を相互に接続して構成される通信ネットワークシステムにおいて、前記複数の通信ネットワークのそれぞれは、通信を行っている特定のユーザを識別する識別番号付きのデータパケットを用いて通信を行い、互いに前記識別番号を独立して管理している複数のネットワークと、請求項１ないし４のうちいずれか１記載の相互接続装置と、他の通信ネットワークの相互接続装置との間を接続し、識別

2

番号なしデータパケットを用いて通信を行う手段とを備えることを特徴とする通信ネットワークシステム。

【請求項６】　複数の通信ネットワーク相互間を相互に接続して構成される通信ネットワークシステムにおいて、前記複数の通信ネットワークのそれぞれは、通信を行っている特定のユーザを識別する識別番号付きのデータパケットを用いて通信を行い、互いに前記識別番号を独立して管理している複数のネットワークと、前記識別番号なしのデータパケットを用いて他の通信ネットワークの相互接続装置との通信を行い、前記識別番号付きのデータパケットを用いて通信を行うネットワークと前記識別番号なしのデータパケットを用いた他の通信ネットワークとを相互に接続する請求項１ないし４のうちいずれか１記載の相互接続装置とを備えることを特徴とする通信ネットワークシステム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、相互接続装置及びこれを用いた通信ネットワークシステムに係り、特に、それぞれが独自の方式で仮想的なプライベートネットワークのサービスを行っている複数のネットワークシステム相互間において、各ネットワークシステム内の独自形式のデータと相互接続用の外部共通形式のデータとの間でデータの変換を行い、それによって各ネットワークシステム相互間でプライベートネットワークの相互接続可能にする相互接続装置及びこれを用いた通信ネットワークシステムに関する。

【０００２】

【従来の技術】近年、急速なネットワークの普及等により、出張先やサテライトオフィスからネットワーク接続サービス事業者（以下、単にサービス事業者という）の回線を通して会社へ接続するという需要が増加している。それに伴い、出張先やサテライトオフィスと会社との間の接続をあたかもローカルエリアネットワークのように扱うことを可能にして、互いに遠隔接続したユーザホスト間の連携を容易にすると共に、それ以外のホストとの間のセキュリティを確保する、いわゆる仮想プライベートネットワーク(Virtual Private Network、以下、ＶＰＮという）が注目されるようになっている。

【０００３】前述のような互いに遠隔地にあるユーザホスト相互間でＶＰＮを構築する方法として、次に説明するような２つの方法が考えられる。第１の方法は、インターネットのような広範囲の地域を網羅しているが信頼性の低い伝送路上で、伝送パケットを暗号化する等により、信頼性のある仮想的な接続を構築するという方法である。第２の方法は、単一のサービス事業者が自らのネットワークを使用した信頼性の高い伝送路内のみにおいて独自のプライベートネットワークサービスを提供している場合、このネットワークを利用するという方法である。このようなネットワークの例として、例えば、ＮＴ

Ｔ　Ｒ&Ｄ１９９８年４月号で紹介されている次世代コネクションレスネットワーク等が知られている。

【０００４】前述の第１の方法は、サービス事業者側がＶＰＮのための機構を導入する必要がほとんどないことや、各ユーザホストが単一のサービス事業者に接続している必要がなく、接続の自由度が高いため、サービス事業者、ユーザ両方にとってネットワーク接続自体のコストが安くなるというメリットを有している。しかし、この第１の方法は、ユーザ側でＶＰＮ構築のためのソフトウェアを導入する必要が有ること、通信時に必ず暗号化・復号化を伴うこと、インターネットの通信品質が保証されていないこと等の理由により、ユーザ側のホスト管理コストや通信品質の点で第２の方法に劣るものである。一方、第２の方法は、逆に、通信品質やホスト管理コストの点で、第１の方法より優れているが、各ユーザホストが単一のサービス事業者に接続しなければならないため、接続できる地理的範囲が限られものである。

【０００５】

【発明が解決しようとする課題】ＶＰＮは、ローカルエリアネットワークを遠隔地へ拡張したものであると考えることができ、可能な限りローカルエリアネットワーク環境に近い、あるいは、それよりも便利な環境を構築することができることが望ましい。このためには、ＶＰＮの環境を、コスト、品質の両面でローカルエリアネットワーク環境に少しでも近づける必要があり、前述した従来技術の欠点の改善が必要である。

【０００６】前述した第１の方法におけるインターネット上の伝送信号を暗号化して伝送する手法の欠点である「ユーザ側のホスト管理コスト」及び「通信品質」の改善方法として、ＶＰＮ用のソフトウェアの設定等の簡易化や、インターネットそのものの通信速度の改善、通信品質の保証を実現することが考えられる。

【０００７】また、前述した第２の方法における単一サービス事業者が提供する独自プライベートネットワークサービスを用いる手法の欠点である「接続できる地理的範囲の制限」については、自らのネットワーク内でＶＰＮサービスを行っており、通信品質について信頼できるサービス事業者の複数の事業者同士が、ユーザの要望に応じてＶＰＮの相互接続を行うという方法によりある程度緩和することができる。

【０００８】しかし、ＶＰＮの実現方法については統一された規格がないため、前述した第２の方法における複数の事業者同士がＶＰＮの相互接続を行ういう方法は、それぞれのサービス事業者側でＶＰＮの仕様が異なることが考えられ、また、両サービス事業者のＶＰＮの仕様が同一の場合でも、ネットワーク管理者がサービス事業者毎に異なるため、各ＶＰＮを一意に識別するために用いているＩＤ番号等が互いに食い違っている場合も考えられるため、単純には相互接続することができないという問題点を有している。

【０００９】一方、前述した第１の方法用いる場合の問題点は、異種ＶＰＮ相互間の中継方法に関する技術として、例えば、特開平１１－４１２８０号公報等に記載された技術により解決されている。しかし、この公報に記載された技術は、１つのサービス事業者が同一のネットワーク上で複数のＶＰＮを提供するという前述した第２の方法が前提としているような場合を想定していないため、第２の方法におけるＶＰＮ相互接続装置として適用することが難しいという問題点を有している。

【００１０】本発明の目的は、前述した第２の方法におけるＶＰＮの仕様やＩＤ番号の相違に関する問題点を解決し、異なるサービス事業者のＶＰＮ相互を効率的に接続することを可能にした相互接続装置及びこれを用いたネットワークシステムを提供することにある。

【００１１】

【課題を解決するための手段】本発明によれば前記目的は、複数のサービス事業者が相手のサービス事業者のネットワークとの接続回線上にＶＰＮ相互接続装置を設置し、サービス事業者内部におけるＶＰＮのＩＤ番号を含んだパケットと、相手のサービス事業者との間で送受信するサービス事業者で統一された形式のパケットとの間で変換を行うようにすることにより達成される。

【００１２】すなわち、本発明によれば前記目的は、特定のユーザに対して仮想的な専用通信路を提供する複数のネットワーク接続サービス事業者のネットワーク同士を相互接続するために、各ネットワーク接続サービス事業者のネットワーク毎に設置される相互接続装置において、前記特定のユーザを識別するために用いられる識別番号が付与されたデータパケットを第１のネットワークインタフェースから受信し、受信したデータパケットを前記識別番号を取り除いたデータパケットに変換し、変換したデータパケットを、相手側ネットワーク接続事業者との接続を行う前記識別番号毎に割り当てられた第２のネットワークインタフェースへ送信する手段と、前記識別番号のないデータパケットを前記第２のネットワークインタフェースから受信し、第２のネットワークインタフェース毎に割り当てられた前記識別番号を受信したデータパケットに付加し、第１のネットワークインタフェースへ送信する手段とを備えることにより達成される。

【００１３】また、前記目的は、複数の通信ネットワーク相互間を相互に接続して構成される通信ネットワークシステムにおいて、前記複数の通信ネットワークのそれぞれは、通信を行っている特定のユーザを識別する識別番号付きのデータパケットを用いて通信を行い、互いに前記識別番号を独立して管理している複数のネットワークと、前述の相互接続装置と、他の通信ネットワークの相互接続装置との間を接続し、識別番号なしデータパケットを用いて通信を行う手段とを備えることにより達成される。

5

【００１４】相互接続装置の相互間は、物理的あるいは論理的に複数の回線が引かれており、この回線の１つ毎に１つのＶＰＮが対応する。このようにすることで、相手のサービス事業者との送受信に使われるパケットにはＶＰＮに関する情報が不用になるので、例えば、一般的なＩＰパケット形式を互いの送受信に用いるパケット形式として採用することができる。さらに、当該するＶＰＮを用いているユーザが常にＩＰのパケット形式を用いて送受信を行っていれば、各サービス事業者はＶＰＮを実現するために付加した余分な情報を取り払うだけでサービス事業者相互送受信用のパケット形式であるＩＰパケットへ変換することができる。

【００１５】

【発明の実施の形態】以下、本発明による相互接続装置及びこれを用いたネットワークシステムの実施形態を図面を用いて詳細に説明する。

【００１６】図１は本発明の相互接続装置を用いてサービス事業者間のＶＰＮ相互接続を行うネットワークシステムの構成例を示すブロック図である。図１において、１００－Ａ、１００－Ｂはサービス事業者ネットワーク、１１０－Ａ、１１０－Ｂは相互接続装置、１２０－Ａ、１２０－Ｂは境界ルータ、１３０はデータ用回線、１４０は管理用回線である。

【００１７】図１（ａ）に示すシステムは、２者のサービス事業者ネットワーク１００－Ａ、１００－Ｂの相互間が各サービス事業者内に置かれた相互接続装置１１０－Ａ、１１０－Ｂにより接続されて構成される。そして、それらの相互接続装置は、各サービス事業者内の境界ルータ１２０－Ａ、１２０－Ｂに第１のネットワークインタフェースとしての回線により接続されている。この図１（ａ）に示す構成は、本発明の実施形態によるネットワークシステムの最も基本的な構成である。図示システムの特徴をなす装置である相互接続装置１１０－Ａと１１０－Ｂとの間は、ＯＳＩ参照モデルにおける物理層あるいはデータリンク層のレベルで個別に分けることができる複数の回線による第２のネットワークインタフェースで接続されている。それらの回線の内の１つは、相互接続装置相互間で各種の設定情報を交換するための管理用回線１４０として使用され、残りの回線は、データ用回線１３０として使用される。境界ルータ１２０－Ａ、１２０－Ｂは、さらに、各サービス事業者ネットワーク内のルータ、サービス事業者がサービス対象とするユーザのネットワーク、他の外部ネットワーク等と接続されるている。

【００１８】相互接続装置１１０－Ａ、１１０－Ｂは、相手のサービス事業者の相互接続装置への中継、あるいは、相手のサービス事業者の相互接続装置からの中継を行うべきＶＰＮを管理し、それらの情報をネットワーク管理者や相手のサービス事業者の相互接続装置へ伝達する。また、相互接続装置１１０－Ａ、１１０－Ｂは、それらのＶＰＮのパケットを境界ルータ１２０－Ａ、１２０－Ｂとの間で送受信できるように境界ルータ間のネットワーク設定を各境界ルータへ送信し、境界ルータや相手の相互接続装置から送られてくる各パケットのうち不正なものを破棄した上で反対側へ中継する。

【００１９】なお、相互接続装置は、受信したパケットをＶＰＮ－ＩＤ（ＶＰＮを一意に識別する番号）及びＶＰＮ－ＩＤと対応させたデータ用回線１３０のみに基づいて転送し、パケットに含まれるＩＰアドレスについては関知しない。このため、ＩＰアドレスに基づくパケットのルーティングは、境界ルータ１２０－Ａ、１２０－Ｂが行う。

【００２０】図１（ｂ）、図１（ｃ）に示す例は、サービス事業者ネットワークを２つ以上とした場合の構成例である。サービス事業者ネットワークを２つ以上とした場合のネットワークシステムは、図１（ｂ）に示すように、各サービス事業者ネットワーク内に接続相手毎に相互接続装置と境界ルータとを備える構成とすることが基本である。また、図１（ｃ）に示すように、２つ以上の接続相手に対して共通の境界ルータを設け、その境界ルータから接続相手毎に別々のネットワークインタフェースを用い、接続相手毎に設けた別々の相互接続装置を介して相手のサービス事業者と接続するという構成であってもよい。但し、いずれの場合も、境界ルータは、受信したデータパケットをその宛先のＩＰアドレスへ向かうネットワークインタフェースのみに対して適切に転送することができる機能を備える必要がある。これは、後述するように、本発明による相互接続装置が、データパケット転送時にＶＰＮ識別番号のみに関与し、データパケットの送信元ＩＰアドレス、宛先ＩＰアドレスについて関知しないことを前提としているためである。

【００２１】図２は本発明の一実施形態による相互接続装置のハードウェア構成を示すブロック図、図３は本発明の一実施形態による相互接続装置のソフトウェア構成を説明する図、図４は本発明の一実施形態による相互接続装置が使用する変換テーブルの構成を説明する図である。図２～図４において、２００はＣＰＵ(Central Processing Unit)、２１０はメモリ、２１３はオペレーティングシステム（ＯＳ）、２１５は制御ソフト、２２０は内部ネットワークコントローラ、２２５は外部ネットワークコントローラ、２３０はキーボードコントローラ、２３５はキーボード、２４０はシリアルコントローラ、２４５はマウス、２５０はディスプレイコントローラ、２５５はディスプレイモニタ、２６０はディスクコントローラ、２６５はディスク装置、３１０は入出力制御部、３２０は変換管理テーブル、３２５は変換テーブル、３３０は境界ルータ接続設定部、３４０はデータ中継部、３５０は管理情報送受信部、３６０は境界ルータ通信部、３７０は外部回線通信部、３８０は内部ネットワークインタフェース部、３９０は外部ネットワークイ

ンタフェース部である。

【００２２】相互接続装置１１０は、図２に示すようなハードウェア構成を持ち、ＣＰＵ２００がメモリ２１０に格納されているプログラムを実行する。メモリ２１０の中には、装置全体を制御するためのＯＳ２１３、相互接続装置としての動作を行うための制御プログラム２１５が格納されている。内部ネットワークコントローラ２２０は、相互接続装置が境界ルータとの間で行う送受信を制御し、外部ネットワークコントローラ２２５は、相互接続装置が相手のサービス事業者の相互接続装置との間で行う送受信を制御する。キーボードコントローラ２３０は、キーボード２３５からのキー入力を制御し、シリアルコントローラ２４０は、シリアルポートに接続されたマウス２４５等の入出力機器を制御する。また、ディスプレイコントローラ２５０は、ディスプレイモニタ２５５への画面表示を制御し、ディスクコントローラ２６０は、ディスク装置２６５への入出力を制御する。

【００２３】図示本発明の実施形態は、ネットワーク管理者による相互接続装置の操作を、装置に直接接続されたキーボード２３５、マウス２４５、ディスプレイモニタ２５５から行うことを前提とするが、相互接続装置とネットワークとを介して接続された遠隔地にある入出力装置を用いて操作を行うことも可能である。

【００２４】制御プログラム２１５内に構成される相互接続装置のソフトウェア構成を図３に示している。図３において、入出力制御部３１０は、キーボード２３５からの入力やディスプレイモニタ２５５への出力を制御する。内部ネットワークインタフェース部３８０は、境界ルータに接続されたネットワークから受信したパケットを境界ルータ通信部３６０に渡したり、境界ルータ通信部３６０からの要求によりパケットをそのネットワークに送信する等の境界ルータとの間の送受信に関する処理を行う。外部ネットワークインタフェース部３９０は、相手のサービス事業者の相互接続装置に接続されたネットワークから受信したパケットを外部回線通信部３７０に渡したり、外部回線通信部３７０から渡されたパケットを要求された通りのネットワークに送信する等の相手の相互接続装置との間の送受信に関する処理を行う。

【００２５】境界ルータ通信部３６０は、内部ネットワークインタフェース部３８０から受け取ったパケットのヘッダを解釈し、その結果に応じて境界ルータ接続設定部３３０、データ中継部３４０のうちの適切な処理モジュールの方へパケットを渡したり、これらの処理モジュールから渡されたパケットに適切なヘッダを付加して内部ネットワークインタフェース部３８０へ渡す等の内部プロトコルに応じたパケットヘッダの解釈と各モジュールへのパケット振分処理とを行う。

【００２６】外部回線通信部３７０は、外部ネットワークインタフェース部３９０から受け取ったパケットをその受信回線に応じて、管理情報送受信部３５０、データ中継部３４０のうちの適切な処理モジュールの方へ渡したり、これらの処理モジュールから渡されたパケットに適切な送信回線の要求を付加して外部ネットワークインタフェース部へ渡す等の外部回線と各モジュールとの間でのパケット振分処理を行う。

【００２７】境界ルータ接続設定部３３０は、境界ルータに与えるべき設定が入出力制御部３１０から管理者により入力されるか、あるいは、管理情報送受信部を通して相手の相互接続装置から与えられると、それらの設定を変換テーブル管理部３２０を通して受け取り、設定情報を境界ルータへ送るための適切な通信手順に基づいてパケットに構築し、境界ルータ通信部３６０へ受け渡す。但し、このような通信による設定手段が境界ルータに備わっていない場合、管理者が手動で境界ルータに設定を行うことによっても対処することができる。

【００２８】管理情報送受信部３５０は、相互接続装置の設定を変換テーブル管理部３２０から得て、相互接続装置間での設定情報交換のためのプロトコルに基づいてパケットを構築し、外部回線通信部３７０へ受け渡す。また、管理情報送受信部３５０は、相互接続装置間の設定交換プロトコルに基づくパケットを外部回線通信部３７０から受け取って解釈し、その設定情報を変換テーブル管理部３２０に受け渡し、さらに場合によっては受信パケットの返答パケットを構築して外部回線通信部３７０へ受け渡す。

【００２９】データ中継部３４０は、境界ルータ通信部３６０から受け取ったパケットに含まれるＶＰＮ－ＩＤを変換テーブル管理部３２０に渡して登録されているか否かを調べ、中継対象として登録されている場合、そのパケットの形式を外部の相互接続装置との間の通信形式であるＩＰパケットに変換し、送出すべきインタフェースの識別子を付加して外部回線通信部３７０に渡す。また、データ中継部３４０は、外部回線通信部３７０からＩＰパケットを受け取ると、そのパケットが流れてきたインタフェースの識別子を変換テーブル管理部３２０に渡して登録されているか否かを調べ、中継対象として登録されている場合、そのパケットの形式を境界ルータとの間の通信形式のパケットに変換し、そのパケット内に変換後のＶＰＮ－ＩＤ番号を書き込んで境界ルータ通信部３６０に渡す。

【００３０】変換テーブル管理部３２０は、変換テーブル３２５を管理し、入出力制御部３１０、境界ルータ接続設定部３３０、データ中継部３４０、管理情報送受信部３５０からの変換テーブル内の情報の追加、削除、検索等の要求を受け付け、それらの要求に基づいて変換テーブルを操作し、検索結果等の返答を要求元モジュールへ返す。

【００３１】変換テーブル３２５には、図４に示すように、各ＶＰＮ－ＩＤのプロトコル変換情報がテーブル形式で格納されている。各変換情報には、ＶＰＮ－ＩＤ４

9

１０、相手ＶＰＮ－ＩＤ４２０、接続ネットマスク４３０、ルータアドレス４４０、相手ルータアドレス４５０、Ｉ／Ｆ識別子４６０、シーケンス番号４７０、フラグ４８０が含まれる。

【００３２】ＶＰＮ－ＩＤ４１０は、この相互接続装置が属するサービス事業者内において、各ＶＰＮを一意に識別するための番号であり、相手ＶＰＮ－ＩＤ４２０は、接続相手のサービス事業者内におけるＶＰＮ－ＩＤである。これらの、ＶＰＮ－ＩＤ４１０で表されるＶＰＮと、相手ＶＰＮ－ＩＤ４２０で表されるＶＰＮとが相互に接続されることとなる。接続ネットマスク４３０は、そのＶＰＮ－ＩＤにおける両者の境界ルータ間のネットワークに割り振るＩＰアドレスのネットマスクであり、ルータアドレス４４０は、そのネットワークにおける境界ルータのＩＰアドレスである。相手ルータアドレス４５０は、そのネットワークにおいて相手のサービス事業者側にある境界ルータのＩＰアドレスである。Ｉ／Ｆ識別子４６０は、そのＶＰＮ－ＩＤにおいて相手の相互接続装置との間で送受信する際に用いるインタフェースの識別子である。シーケンス番号４７０は、相互接続装置同士が交換した管理メッセージを一意に識別するためのシーケンス番号を一時的に格納するために用いられる。フラグ４８０は、管理メッセージの交換状態を表すために用いられる状態フラグであり、フラグ４８０が表す状態には、「仮登録返答待ち」、「登録完了待ち」、「登録承認待ち」、「削除承認待ち」、「有効」の５種類がある。相互接続装置は、受信したパケットのＶＰＮ－ＩＤが「有効」として変換テーブルに登録されている場合にのみ、そのパケットの転送を行う。

【００３３】なお、前述したテーブルの内容、特に、ＶＰＮ－ＩＤの識別番号と相手側相互接続装置に接続される回線を示すＩ／Ｆ識別子のネットワークインタフェースとの対応関係等については、管理者が入出力装置を通して、あるいは、管理者が操作する図示しない装置との間で通信を行って、追加または削除することができる。また、管理者は、他のネットワーク接続サービス事業者のネットワークに設置された相互接続装置から受信した前述の情報を確認し、入出力装置を通して、あるいは、管理者が操作する図示しない装置との間で通信を行って、これを設定することを承認するようにすることができる。

【００３４】図５は相互接続装置相互間のＶＰＮ変換情報の登録シーケンスを示しており、以下、これについて説明する。図５に示すシーケンスは、相互接続装置１１０－Ａ側のネットワーク管理者の要求による登録処理を示しているが、相互接続装置１１０－Ｂ側からの要求の場合も同様である。

【００３５】（１）要求を出す相互接続装置１１０－Ａ側のネットワーク管理者は、互いに接続したい相互接続装置１１０－Ａ側のＶＰＮ－ＩＤ、相互接続装置１１０

10

－Ｂ側のＶＰＮ－ＩＤ、境界ルータ間の相互接続に利用できるＩＰネットワークアドレスを予め把握していることとする。まず、ネットワーク管理者は、相互接続装置１１０－Ａに対して変換の対象となるＶＰＮ－ＩＤ、相手ＶＰＮ－ＩＤ、接続ネットマスク、境界ルータ１２０－Ａのルータアドレス、及び、相互接続装置１１０－ＡのＩ／Ｆ識別子を入力する（シーケンス５００）。

【００３６】（２）相互接続装置１１０－Ａは、入力された情報を、フラグを「仮登録返答待ち」にして変換テーブル３２５に仮登録する。そして、それらの情報を含むＶＰＮ登録メッセージを相互接続装置Ｂへ管理用回線を通して送信する（シーケンス５１０）。

【００３７】（３）このメッセージを受信した相互接続装置１１０－Ｂは、自らの変換テーブルへ受信した送信側ＶＰＮ－ＩＤ、受信側ＶＰＮ－ＩＤ、接続ネットマスク、送信側ルータアドレスを、フラグを「登録承認待ち」にして仮登録する。また、相互接続装置１１０－Ｂは、相手の相互接続装置のＩ／Ｆ識別子から、その回線に接続されている自らのＩ／Ｆ識別子を導き出し、仮登録した変換情報のＩ／Ｆ識別子フィールドに登録する。相互接続装置１１０－Ｂは、相互接続装置１１０－Ａから要求されたＶＰＮ変換情報の仮登録処理が終わると、相互接続装置１１０－Ａに対して管理用回線を通して仮登録完了を表すＡＣＫメッセージを送信する（シーケンス５２０）。

【００３８】（４）このメッセージを受信した相互接続装置１１０－Ａは、対象となる変換情報のフラグを「登録完了待ち」へ変更する。その後、相互接続装置１１０－Ｂは、仮登録された変換情報の登録承認及び追加情報の入力が相互接続装置１１０－Ｂ側のネットワーク管理者によって行われるまで待ち状態となる。但し、データパケットの変換処理及び他のＶＰＮに関する変換情報登録、削除の処理については、この入力待ちとは無関係に並行して処理することができる（シーケンス５３０）。

【００３９】（５）相互接続装置１１０－Ｂは、シーケンス５３０により相互接続装置１１０－Ｂ側のネットワーク管理者によってＶＰＮ変換情報設定の登録承認及び境界ルータ１２０－Ｂのルータアドレスが入力されると、次のシーケンス以降の処理に移る。但し、相互接続装置１１０－Ａ側と１１０－Ｂ側のネットワーク管理者が同一の場合、シーケンス５３０及びその入力待ち処理を省略し、境界ルータ１２０－Ｂのルータアドレスも相互接続装置１１０－Ａ側のネットワーク管理者がシーケンス５００で与えるようにすることができる。シーケンス５３０でネットワーク管理者による承認が与えられると、相互接続装置１１０－Ｂは、まず、境界ルータＢに対してアドレス設定等のデータの送受信やルーティングプロトコルの交換に必要な設定を行う。但し、この設定を相互接続装置１１０－Ｂが自動的に行うことができない場合、ネットワーク管理者が直接境界ルータ１２０－

Ｂに対してこれらの設定を行ってもよい（シーケンス５４０）。

【００４０】（６）境界ルータ１２０－Ｂに対するシーケンス５４０での設定が終わると、相互接続装置１１０－Ｂは、変換テーブル内の該当する変換情報のフラグを「有効」へ変更し、登録完了メッセージを相互接続装置１１０－Ａに対して管理用回線を通して送信する（シーケンス５５０）。

【００４１】（７）登録完了メッセージを受信した相互接続装置１１０－Ａは、境界ルータ１２０－Ａに対してアドレス設定等のデータ送受信やルーティングプロトコルの交換に必要な設定を行う。但し、この設定を相互接続装置１１０－Ａが自動的に行うことができない場合、ネットワーク管理者が直接境界ルータ１２０－Ａに対してこれらの設定を行ってもよい（シーケンス５６０）。

【００４２】（８）相互接続装置１１０－Ａは、境界ルータ１２０－Ａに対するシーケンス５６０での設定が終わると、変換テーブル内の該当する変換情報のフラグを「有効」へ変更し、相互接続装置１１０－Ｂに対してへ管理用回線を通して登録完了を表すＡＣＫメッセージを送信する（シーケンス５７０）。

【００４３】図６は相互接続装置相互間のＶＰＮ変換情報の削除シーケンスを示しており、以下、これについて説明する。図６に示すシーケンスは、相互接続装置１１０－Ａ側のネットワーク管理者の要求による削除処理を示しているが、相互接続装置１１０－Ｂ側からの要求の場合も同様である。

【００４４】（１）要求を出す相互接続装置１１０－Ａ側のネットワーク管理者は、まず、相互接続装置１１０－Ａに対して、変換テーブルから削除したいＶＰＮ－ＩＤを入力する。相互接続装置１１０－Ａは、入力されたＶＰＮ―ＩＤと一致する変換情報を変換テーブルから検索し、見つかった変換情報に基づいて境界ルータ１２０－Ａに対してアドレス削除等のデータ送受信やルーティングプロトコルの交換の中止に必要な設定を行う。但し、この設定を相互接続装置１１０－Ａが自動的に行うことができない場合、ネットワーク管理者が直接境界ルータ１２０－Ａに対してこれらの設定を行ってもよい（シーケンス６００、６１０）。

【００４５】（２）シーケンス６１０の処理後、相互接続装置１１０－Ａは、該当するＶＰＮ－ＩＤの削除メッセージを相互接続装置１１０－Ｂに対して管理用回線を通して送信し、該当する変換情報を変換テーブルから削除する（シーケンス６２０）。

【００４６】（３）シーケンス６２０によるメッセージを受信した相互接続装置１１０－Ｂは、自らの変換テーブルから受信した受信側ＶＰＮ－ＩＤを検索し、見つかった変換情報のフラグを「削除承認待ち」にすることによって変換情報を仮削除し、相互接続装置１１０－Ａに対して管理用回線を通して仮削除完了を表すＡＣＫメッセージを送信する（シーケンス６３０）。

【００４７】（４）その後、相互接続装置１１０－Ｂは、仮削除された変換情報の削除承認が相互接続装置Ｂ側のネットワーク管理者によって行われるまで入力待ち状態となる。但し、データパケットの変換処理及び他ＶＰＮに関する変換情報の登録処理、削除処理については、この入力待ちとは無関係に並行して処理することができる（シーケンス６４０）。

【００４８】（５）相互接続装置１１０－Ｂは、シーケンス６４０により削除の承認が入力されると、次のシーケンスの処理に移る。但し、相互接続装置１１０－Ａ側と１１０－Ｂ側とのネットワーク管理者が同一の場合、シーケンス６４０及びその入力待ち処理を省略することができる。シーケンス６４０でネットワーク管理者による承認が与えられると、相互接続装置１１０－Ｂは、境界ルータ１２０－Ｂに対してアドレス削除等のデータ送受信やルーティングプロトコルの交換の中止に必要な設定を行う。但し、この設定を相互接続装置１１０－Ｂが自動的に行うことができない場合、ネットワーク管理者が直接境界ルータＢに対してこれらの設定を行ってもよい。境界ルータ１２０－Ｂに対する設定が終了すると、相互接続装置１１０－Ｂは、変換テーブル内の該当する変換情報を完全に削除する（シーケンス６５０）。

【００４９】図７は相互接続装置相互間でのデータパケットの送受信シーケンスを示しており、以下、これについて説明する。図７に示すシーケンスは、相互接続装置１１０－Ａ側からのデータパケットの送信処理を示しているが、相互接続装置１１０－Ｂ側からの送信の場合も同様である。

【００５０】（１）相互接続装置１１０－Ａは、境界ルータ１２０－Ａから送信すべきパケットを受け取ると、そのヘッダに含まれるＶＰＮ－ＩＤを変換テーブルから検索する。その結果、変換テーブルに該当する変換情報が存在し、かつ、そのフラグが「有効」であるならば、そのデータパケットからサービス事業者内部での送受信のために付けられているヘッダ（ＶＰＮ－ＩＤを含む）を取り除いて、相互接続装置１１０－Ｂに対してＶＰＮ－ＩＤに対応するデータ用回線を用いて送信する（シーケンス７００、７１０）。

【００５１】（２）相互接続装置１１０－Ａからデータパケットを受信した相互接続装置１１０－Ｂは、受信したデータ用回線のＩ／Ｆ識別子を変換テーブルから検索する。その結果、該当する変換情報が存在し、かつ、そのフラグが「有効」であるならば、その変換情報のＶＰＮ－ＩＤを含むサービス事業者内部用ヘッダをそのパケットに付加し、境界ルータ１２０－Ｂへ転送する（シーケンス７２０）。

【００５２】図８はＶＰＮ変換情報を登録しようとしたサービス事業者側の相互接続装置が他方の相互接続装置へ送信する登録メッセージの形式を示す図であり、図５

により説明したシーケンス５１０で送信されるメッセージである。

【００５３】図８に示すように、登録メッセージ８００は、メッセージ長等を含むメッセージヘッダであるヘッダ８０５と、以下に説明する各種の情報８１０～８７０により構成される。シーケンス番号８１０は、管理用回線を流れる各メッセージを一意に区別するための番号で、今までに流れたメッセージのシーケンス番号と可能な限り異なる値が用いられる。送信側外部Ｉ／Ｆ識別子８２０は、このメッセージを送信する側の相互接続装置における該当ＶＰＮ－ＩＤに対応するインタフェース識別子である。送信側内部ＶＰＮ－ＩＤ８３０は、このメッセージを送信する側のサービス事業者内におけるＶＰＮ－ＩＤである。受信側内部ＶＰＮ－ＩＤ８４０は、このメッセージを受信する側のサービス事業者内におけるＶＰＮ－ＩＤである。最終的に、この送信側内部ＶＰＮ－ＩＤ８３０で表されるＶＰＮと受信側内部ＶＰＮ－ＩＤ８４０で表されるＶＰＮ同士が互いに接続されることになる。ルータ間接続ＩＰネットマスク８５０は、境界ルータ間のネットワークのＩＰネットマスクである。送信側ルータＩＰアドレス８６０は、境界ルータ間の接続において送信側の境界ルータに割り当てたＩＰアドレスである。受信側ルータＩＰアドレス８７０は、境界ルータ間の接続において受信側の境界ルータに割り当てるＩＰアドレスである。但し、受信側のネットワーク管理者が受信側の境界ルータに割り当てるＩＰアドレスを決定する場合、この受信側ルータＩＰアドレスのフィールドは空でもよい。

【００５４】図９は登録メッセージを受信した相互接続装置が登録メッセージを送信してきた相互接続装置へ返信する登録完了メッセージの形式を示す図であり、図５により説明したシーケンス５５０で送信されるメッセージである。

【００５５】図９に示すように、登録完了メッセージ９００は、メッセージ長等を含むメッセージヘッダであるヘッダ９０５と、以下に説明する各種の情報９１０～９７０により構成される。

【００５６】シーケンス番号９１０は、管理用回線を流れる各メッセージを一意に区別するための番号で、今までに流れたメッセージのシーケンス番号と可能な限り異なる値が用いられる。仮設定シーケンス番号９２０は、このメッセージが返答の対象としている登録メッセージのシーケンス番号である。送信側内部ＶＰＮ－ＩＤ９３０は、このメッセージを送信する側のサービス事業者内におけるＶＰＮ－ＩＤである。受信側内部ＶＰＮ－ＩＤ９４０は、このメッセージを受信する側のサービス事業者内におけるＶＰＮ－ＩＤである。この送信側内部ＶＰＮ－ＩＤ９３０で表されるＶＰＮと受信側内部ＶＰＮ－ＩＤ９４０で表されるＶＰＮ同士が互いに接続されたことになる。ルータ間接続ＩＰネットマスク９５０は、境界ルータ間のネットワークのＩＰネットマスクである。送信側ルータＩＰアドレス９６０は、境界ルータ間の接続において送信側の境界ルータに割り当てたＩＰアドレスである。受信側ルータＩＰアドレス９７０は、境界ルータ間の接続において受信側の境界ルータに割り当てたＩＰアドレスである。

【００５７】図１０はＶＰＮ変換情報を削除しようとしたサービス事業者側の相互接続装置が他方の相互接続装置へ送信する削除メッセージの形式を示す図であり、図６により説明したシーケンス６２０で送信されるメッセージである。

【００５８】図１０に示すように、削除メッセージ１０００は、メッセージ長等を含むメッセージヘッダであるヘッダ１００５と、管理用回線を流れる各メッセージを一意に区別するための番号で、今までに流れたメッセージのシーケンス番号と可能な限り異なる値が用いられるシーケンス番号１０１０と、このメッセージを受信する側のサービス事業者内におけるＶＰＮ－ＩＤである受信側内部ＶＰＮ－ＩＤ１０２０とにより構成される。そして、ＶＰＮ－ＩＤで指定された変換情報が両側の相互接続装置の変換テーブルから削除される。

【００５９】図１１は図８～図１０のメッセージを受け取った相互接続装置が相手の相互接続装置へ返答する受信確認（ＡＣＫ）メッセージの形式を示す図である。

【００６０】ＡＣＫメッセージ１１００は、メッセージ長等を含むメッセージヘッダであるヘッダ１１０５と、このＡＣＫメッセージが返答の対象としているメッセージのシーケンス番号である返答対象シーケンス番号１１１０と、このメッセージを受信する側のサービス事業者内におけるＶＰＮ－ＩＤである受信側内部ＶＰＮ－ＩＤ１１２０とにより構成される。ＡＣＫメッセージは、返答対象メッセージのシーケンス番号のみを持ち、ＡＣＫメッセージ自身のシーケンス番号を持たない。そして、前述の受信側内部ＶＰＮ－ＩＤ１１２０は、返答対象のメッセージが指定したＶＰＮ－ＩＤと対応させられている。

【００６１】図１２は相互接続装置がメッセージの受け取り時にエラーが発生した場合に相手の相互接続装置へ送信する異常通知（ＮＯＴＩＦＹ）メッセージの形式を示す図である。

【００６２】ＮＯＴＩＦＹメッセージ１２００は、メッセージ長等を含むメッセージヘッダであるヘッダ１２０５と、管理用回線を流れる各メッセージを一意に区別するための番号で、今までに流れたメッセージのシーケンス番号と可能な限り異なる値が用いられるシーケンス番号１２１０と、このメッセージを受信する側のサービス事業者内におけるＶＰＮ－ＩＤである受信側内部ＶＰＮ－ＩＤ１２２０と、このＮＯＴＩＦＹメッセージが相手の相互接続装置へ伝えるエラーの種別を表すエラーコード１２３０と、エラーの内容を表すための付加的なパラ

メータであるエラーパラメータ１２４０とにより構成される。前述の受信側内部ＶＰＮ－ＩＤ１２２０は、このＮＯＴＩＦＹメッセージがエラーの対象とするＶＰＮ－ＩＤと対応させられている。

【００６３】図１３はＶＰＮ変換情報を登録しようとしたサービス事業者側の相互接続装置における変換情報仮登録の処理動作を説明するフローチャートであり、以下、これについて説明する。この処理は、前述の図５のシーケンス５００でネットワーク管理者の登録要求を受け取った相互接続装置１１０－Ａが、フラグを「仮登録返答待ち」にして、入力された情報を変換テーブル３２５に仮登録し、シーケンス５１０で登録メッセージを送信するまでの処理に相当する。

【００６４】（１）ネットワーク管理者からＶＰＮ変換情報の新規登録要求が入力された相互接続装置は、自ＶＰＮ－ＩＤが一致する変換情報を変換テーブルから検索し、検索の結果、要求されたＶＰＮ－ＩＤが自装置の変換テーブルにすでに登録されているか否かチェックする（ステップ１３０５、１３１０）。

【００６５】（２）ステップ１３１０のチェックで、もし変換テーブルに要求されたＶＰＮ－ＩＤがあれば、ネットワーク管理者が使用しているディスプレイモニタへエラーを出力してここでの処理を終了す（ステップ１３２５）。

【００６６】（３）ステップ１３１０のチェックで、変換テーブルに要求されたＶＰＮ－ＩＤがなければ、ネットワーク管理者によって入力された自サービス事業者側の変換対象ＶＰＮ－ＩＤ、相手サービス事業者側のＶＰＮ－ＩＤ、境界ルータ間接続のＩＰネットマスク、自サービス事業者側の境界ルータのＩＰアドレス、及び、自サービス事業者側相互接続装置のＩ／Ｆ識別子を変換テーブルへ新たな変換情報として登録する。さらに、その変換情報のシーケンス番号に、後のステップ１３２０で送信する登録メッセージのシーケンス番号を登録し、フラグに、「仮登録返答待ち」を表すフラグ値を登録する（ステップ１３１５）。

【００６７】（４）そして、各フィールドにステップ１３１５で登録したものと同じ値を持つ登録メッセージ（但し、相手サービス事業者側のルータＩＰアドレスがネットワーク管理者から指定された場合は、そのフィールドもさらに含む）を相手サービス事業者側の相互接続装置に対して管理用回線経由で送信してここでの処理を終了する（ステップ１３２０）。

【００６８】図１４はＶＰＮ変換情報を削除しようとしたサービス事業者側の相互接続装置における変換情報削除の処理動作を説明するフローチャートであり、以下、これについて説明する。この処理は、図６において、シーケンス６００でネットワーク管理者の削除要求を受け取った相互接続装置１１０－Ａが、シーケンス６２０で削除メッセージを送信し、削除を要求された情報を変換テーブル３２５から削除するまでの処理に相当する。

【００６９】（１）ネットワーク管理者からＶＰＮ変換情報の削除要求を入力された相互接続装置は、自ＶＰＮ－ＩＤが一致する変換情報を変換テーブルから検索し、検索の結果、要求されたＶＰＮ－ＩＤがすでに変換テーブルに登録されているか否かをチェックする（ステップ１４０５、１４１０）。

【００７０】（２）ステップ１４１０のチェックで、もし変換テーブルに要求されたＶＰＮ－ＩＤがなければ、ネットワーク管理者が使用しているディスプレイモニタへエラーを出力してここでの処理を終了す（ステップ１４３０）。

【００７１】（３）ステップ１４１０のチェックで、変換テーブルに要求されたＶＰＮ－ＩＤがあれば、自サービス事業者側の境界ルータに対して、変換情報に含まれる各種情報（自サービス事業者側と相手サービス事業者側の境界ルータのＩＰアドレス、境界ルータ間接続のＩＰネットマスク）やその他ルーティング情報交換のための設定の解除要求を送信する。但し、自サービス事業者側の境界ルータが相互接続装置からの設定送信による設定変更に対応できない場合、ネットワーク管理者が削除要求入力を行う前に、他の手段で境界ルータに対して直接この設定解除を行ってもよい（ステップ１４１５）。

【００７２】（４）次に、対象となっている変換情報に登録されている相手ＶＰＮ－ＩＤを受信側内部ＶＰＮ－ＩＤに持つ削除メッセージを、相手サービス事業者側の相互接続装置へ管理用回線経由で送信し、対象となっている変換情報を完全に削除してここでの処理を終了する（ステップ１４２０、１４２５）。

【００７３】図１５は登録メッセージを受信した相互接続装置における変換情報仮登録の処理動作を説明するフローチャートであり、以下、これについて説明する。この処理は、例えば、前述した図５において、相互接続装置１１０－Ｂが、シーケンス５１０で登録メッセージを受信してからシーケンス５２０でＡＣＫメッセージを送信するまでの処理に相当する。

【００７４】（１）相手サービス事業者側の相互接続装置から登録メッセージを受信した相互接続装置は、そのメッセージに含まれる受信側ＶＰＮ－ＩＤに一致する変換情報を変換テーブルから検索し、検索の結果、要求された受信側ＶＰＮ－ＩＤが自装置の変換テーブルにすでに登録されているか否かチェックする（ステップ１５０５、１５１０）。

【００７５】（２）ステップ１５１０のチェックで、もし変換テーブルに要求された受信側ＶＰＮ－ＩＤがあれば、相手サービス事業者側の相互接続装置へ、エラーを表すＮＯＴＩＦＹメッセージを送信してここでの処理を終了す（ステップ１５２５）。

【００７６】（３）ステップ１５１０のチェックで、変換テーブルに要求された受信側ＶＰＮ－ＩＤがなけれ

ば、登録メッセージに含まれる送信側の変換対象ＶＰＮ－ＩＤ、受信側のＶＰＮ－ＩＤ、境界ルータ間接続のＩＰネットマスク、送信側の境界ルータのＩＰアドレスを変換テーブルへ新たな変換情報として登録する。さらに、その変換情報のＩ／Ｆ識別子に、メッセージ内に含まれる送信側外部Ｉ／Ｆ識別子から導き出した受信側相互接続装置のＩ／Ｆ識別子を登録し、シーケンス番号に、登録メッセージのシーケンス番号を登録し、フラグに、「登録承認待ち」を表すフラグ値を登録する（ステップ１５１５）。

【００７７】（４）そして、仮登録完了を表すＡＣＫメッセージを相手サービス事業者側の相互接続装置にたいして管理用回線経由で送信してここでの処理を終了する（ステップ１５２０）。

【００７８】図１６は削除メッセージを受信した相互接続装置における変換情報仮削除の処理動作を説明するフローチャートであり、以下、これについて説明する。この処理は、図６において、相互接続装置１１０－Ｂが、シーケンス６２０で削除メッセージを受信してからシーケンス６３０でＡＣＫメッセージを送信するまでの処理に相当する。

【００７９】（１）相手サービス事業者側の相互接続装置から削除メッセージを受信した相互接続装置は、そのメッセージに含まれる受信側ＶＰＮ－ＩＤが変換テーブルにすでに登録されているか否かを検索し、検索の結果、削除すべき受信側ＶＰＮ－ＩＤがすでに変換テーブルに登録されているか否かをチェックする（ステップ１６０５、１６１０）。

【００８０】（２）ステップ１６１０のチェックで、もし変換テーブルに受信側ＶＰＮ－ＩＤがなければ、相手サービス事業者側の相互接続装置へ未登録エラーを表すＮＯＴＩＦＹメッセージを出力してここでの処理を終了する（ステップ１６２５）。

【００８１】（３）ステップ１６１０のチェックで、変換テーブルに受信側ＶＰＮ－ＩＤがあれば、検索によって見つかった変換情報のフラグを「削除承認待ち」に変更し、そして、仮削除完了を表すＡＣＫメッセージを相手サービス事業者側の相互接続装置に対して管理用回線経由で送信して処理を終了する（ステップ１６１５、１６２０）。

【００８２】図１７は管理者の登録承認を受けた相互接続装置における変換情報登録完了の処理動作を説明するフローチャートであり、以下、これについて説明する。この処理は、例えば、前述した図５において、相互接続装置１１０－Ｂが、シーケンス５３０で管理者の登録承認を受けてからシーケンス５５０で登録完了メッセージを送信するまでの処理に相当する。

【００８３】（１）ネットワーク管理者による登録承認を入力された相互接続装置は、その入力に含まれる自サービス事業者側ＶＰＮ－ＩＤが変換テーブルにすでに登録されているか否かを検索し、検索の結果、自サービス事業者側ＶＰＮ－ＩＤがすでに変換テーブルに登録されているか否かをチェックする（ステップ１７０５、１７１０）。

【００８４】（２）ステップ１７１０のチェックで、もし変換テーブルに自サービス事業者側ＶＰＮ－ＩＤがなければネットワーク管理者が使用しているディスプレイモニタへエラーを出力してここでの処理を終了する（ステップ１７４０）。

【００８５】（３）ステップ１７１０のチェックで、変換テーブルに自サービス事業者側ＶＰＮ－ＩＤがあれば、見つかったその変換情報のフラグが「登録承認待ち」になっているか否かをチェックし、フラグが「登録承認待ち」でなければネットワーク管理者が使用しているディスプレイモニタへエラーを出力してここでの処理を終了する（ステップ１７１５、１７４０）。

【００８６】（４）ステップ１７１５のチェックで、見つかった変換情報のフラグが「登録承認待ち」であれば、見つかった変換情報の登録承認時に入力された自サービス事業者側の境界ルータのＩＰアドレス及び自サービス事業者側相互接続装置のＩ／Ｆ識別子をその変換情報に登録する。但し、自サービス事業者側の境界ルータのＩＰアドレスについては、管理者による入力時に変更が特になければ、相手サービス事業者側の相互接続装置から送られてきた値がそのまま使用される。また、境界ルータのＩＰアドレスとＩ／Ｆ識別子とについては、相互接続装置が適切な値を自動的に決定してもよい（ステップ１７２０）。

【００８７】（５）次に、自サービス事業者側の境界ルータに対して、自サービス事業者側と相手サービス事業者側との境界ルータのＩＰアドレス、境界ルータ間接続のＩＰネットマスク、その他ルーティング情報交換のための設定を送信する。但し、自サービス事業者側の境界ルータが相互接続装置からの設定送信による設定変更に対応できない場合、ネットワーク管理者が登録承認入力を行う前に、他の手段により境界ルータに対して直接この設定を行ってもよい（ステップ１７２５）。

【００８８】（６）そして、対象となっている変換情報のフラグを「有効」に変更し、相手サービス事業者側の相互接続装置へ登録完了メッセージを送信する。この登録完了メッセージの各フィールドには、対象となっている変換情報の各フィールドの値を用いる（ステップ１７３０、１７３５）。

【００８９】図１８は管理者の削除承認を受けた相互接続装置における変換情報削除完了の処理動作を説明するフローチャートであり、以下、これについて説明する。この処理は、例えば、図６において、相互接続装置１１０－Ｂが、シーケンス６４０で管理者の削除承認を受けてから、削除を要求された情報を変換テーブル３２５から削除するまでの処理に相当する。

【００９０】（１）ネットワーク管理者による削除承認が入力された相互接続装置は、その入力に含まれる自サービス事業者側ＶＰＮ－ＩＤが変換テーブルにすでに登録されているか否かを検索し、検索の結果、自サービス事業者側ＶＰＮ－ＩＤがすでに変換テーブルに登録されているか否かをチェックする（ステップ１８０５、１８１０）。

【００９１】（２）ステップ１８１０のチェックで、もし変換テーブルに自サービス事業者側ＶＰＮ－ＩＤがなければネットワーク管理者が使用しているディスプレイモニタへエラーを出力してここでの処理を終了する（ステップ１８３０）。

【００９２】（３）ステップ１８１０のチェックで、変換テーブルに自サービス事業者側ＶＰＮ－ＩＤがあれば、見つかったその変換情報のフラグが「削除承認待ち」か否かをチェックし、フラグが「削除承認待ち」でなければネットワーク管理者が使用しているディスプレイモニタへエラーを出力してここでの処理を終了する（ステップ１８１５、１８３０）。

【００９３】（４）ステップ１８１５のチェックで、フラグが「削除承認待ち」であれば、自サービス事業者側の境界ルータに対して、変換情報に含まれる各種情報（自サービス事業者側と相手サービス事業者側の境界ルータのＩＰアドレス、境界ルータ間接続のＩＰネットマスク）やその他ルーティング情報交換のための設定の解除要求を送信する。但し、自サービス事業者側の境界ルータが相互接続装置からの設定送信による設定変更に対応できない場合、ネットワーク管理者が削除承認入力を行う前に、他の手段で境界ルータに対して直接この設定解除を行ってもよい（ステップ１８２０）。

【００９４】（５）そして、ネットワーク管理者による削除承認が入力された相互接続装置は、対象となっている変換情報を完全に削除して処理を終了する（ステップ１８２５）。

【００９５】図１９は登録完了メッセージを受信した相互接続装置における変換情報登録完了の処理動作を説明するフローチャートであり、以下、これについて説明する。この処理は、例えば、前述した図５において、相互接続装置１１０－Ａが、シーケンス５５０で登録完了メッセージを受信してからシーケンス５７０でＡＣＫメッセージを送信するまでの処理に相当する。

【００９６】（１）相手サービス事業者側の相互接続装置から登録完了メッセージを受信した相互接続装置は、その入力に含まれる自サービス事業者側ＶＰＮ－ＩＤが変換テーブルにすでに登録されているか否かを検索し、検索の結果、自サービス事業者側ＶＰＮ－ＩＤがすでに変換テーブルに登録されているか否かをチェックする（ステップ１９０５、１９１０）。

【００９７】（２）ステップ１９１０のチェックで、もし変換テーブルに自サービス事業者側ＶＰＮ－ＩＤがなければ、相手サービス事業者側の相互接続装置へ「該当する登録完了待ち変換情報なし」のエラーを表すＮＯＴＩＦＹメッセージを出力してここでの処理を終了する（ステップ１９４５）。

【００９８】（３）また、ステップ１９１０のチェックで、変換テーブルに自サービス事業者側ＶＰＮ－ＩＤがあれば、見つかった変換情報のフラグが「登録完了待ち」か否かをチェックし、フラグが「登録完了待ち」でなければ、前述と同様にＮＯＴＩＦＹメッセージを出力してここでの処理を終了する（ステップ１９１５、１９４５）。

【００９９】（４）また、ステップ１９１５のチェックで、フラグが「登録完了待ち」であれは、見つかった変換情報のシーケンス番号が受信した登録完了メッセージ内の仮設定シーケンス番号と一致するか否かをチェックし、一致しなければ、前述と同様にＮＯＴＩＦＹメッセージを出力してここでの処理を終了する（ステップ１９２０、１９４５）。

【０１００】（５）ステップ１９２０のチェックで、見つかった変換情報のシーケンス番号が受信した登録完了メッセージ内の仮設定シーケンス番号と一致した場合、すなわち、ステップ１９１０、１９１５、１９２０のチェックにより該当する変換情報が見つかった場合、受信した登録完了メッセージに含まれる送信側の境界ルータのＩＰアドレスと、該当する変換情報の相手サービス事業者側境界ルータのＩＰアドレスとを比較する。その結果、値が異なるか、あるいは変換情報側のこれらのフィールドが未登録である場合、メッセージ内のこれらの値を変換情報側へコピーして、相手側境界ルータのＩＰアドレスを登録し、対象となっている変換情報のフラグを「有効」に変更する（ステップ１９２５、１９３０）。

【０１０１】（６）次に、自サービス事業者側の境界ルータに対して、自サービス事業者側と相手サービス事業者側との境界ルータのＩＰアドレス、境界ルータ間接続のためのＩＰネットマスク、その他ルーティング情報交換のための設定を送信する。但し、自サービス事業者側の境界ルータが相互接続装置からの設定送信による設定変更に対応できない場合、ネットワーク管理者が図１３の仮登録処理の前に行った登録要求入力を行う前に、他の手段により境界ルータに対して直接この設定を行ってもよい（ステップ１９３５）。

【０１０２】（７）最後に、登録完了を表すＡＣＫメッセージを相手サービス事業者側の相互接続装置へ管理用回線経由で送信して処理を終了する（ステップ１９４０）。

【０１０３】図２０はＡＣＫメッセージを受信した相互接続装置における各種の処理動作を説明するフローチャートであり、以下、これについて説明する。この処理は、図５のシーケンス５２０及び５７０、あるいは、図６のシーケンス６３０で送信されたＡＣＫメッセージを

受け取った相互接続装置の処理である。

【０１０４】（１）相手サービス事業者側の相互接続装置からＡＣＫメッセージを受信した相互接続装置は、受信したＡＣＫメッセージに含まれる自サービス事業者側ＶＰＮ－ＩＤが変換テーブルにすでに登録されているか否かを検索し、検索の結果、自サービス事業者側ＶＰＮ－ＩＤがすでに変換テーブルに登録されているか否かをチェックする（ステップ２００５、２０１０）。

【０１０５】（２）ステップ２０１０のチェックで、もし変換テーブルに自サービス事業者側ＶＰＮ－ＩＤがなければ、相手サービス事業者側の相互接続装置へ「該当する変換情報なし」のエラーを表すＮＯＴＩＦＹメッセージを出力してここでの処理を終了する。（ステップ２０２５）。

【０１０６】（３）また、ステップ２０１０のチェックで、変換テーブルに自サービス事業者側ＶＰＮ－ＩＤがあれば、その変換情報のシーケンス番号が受信したＡＣＫメッセージ内の返答対象シーケンス番号と一致するか否かをチェックし、一致しなければ、前述と同様にＮＯＴＩＦＹメッセージを出力してここでの処理を終了する（ステップ２０１５、２０２５）。

【０１０７】（４）ステップ２０１５のチェックで、変換情報のシーケンス番号が受信したＡＣＫメッセージ内の返答対象シーケンス番号と一致すれば、その変換情報のフラグが「仮登録返答待ち」か否かをチェックし、フラグが「仮登録返答待ち」でなければ、何も行わずにこの処理を終了する（ステップ２０２０）。

【０１０８】（５）ステップ２０２０のチェックで、フラグが「仮登録返答待ち」であれば、そのフラグを「登録完了待ち」に変更して処理を終了する（ステップ２０３０）。

【０１０９】図２１は自サービス事業者側からデータパケットを受信した相互接続装置がそのパケットを外部に送信する外部送信処理の動作を説明するフローチャートであり、以下、これについて説明する。この処理は、図７に示すシーケンス７００、７１０により説明した境界ルータ１２０－Ａからのデータパケットを受信した相互接続装置１１０－Ａが、相互接続装置１１０－Ｂにパケットを送信する処理である。

【０１１０】（１）境界ルータからデータパケットを受信した相互接続装置は、そのデータパケットの先頭に置かれている自サービス事業者内通信用ヘッダを見て、そのヘッダに含まれるＶＰＮ－ＩＤが変換テーブルにすでに登録されているか否かをを検索し、検索の結果、そのＶＰＮ－ＩＤがすでに変換テーブルに登録されているか否かをチェックする（ステップ２１０５、２１１０）。

【０１１１】（２）ステップ２１１０のチェックで、もし変換テーブルに該当ＶＰＮ－ＩＤがなければ、そのパケットを破棄してここでの処理を終了する（ステップ２１３０）。

【０１１２】（３）また、ステップ２１１０のチェックで、変換テーブルに該当ＶＰＮ－ＩＤがあれば、その変換情報のフラグが「有効」か否かをチェックし、フラグが「有効」でなければ、前述と同様にパケットを破棄してここでの処理を終了する（ステップ２１１５、２１３０）。

【０１１３】（４）ステップ２１１５のチェックで、変換情報のフラグが有効であれば、そのパケットから自サービス事業者内通信用ヘッダを取り除いてＩＰパケットを取り出し、そのＩＰパケットを検索によって見つかった変換情報に含まれるＩ／Ｆ識別子で表されるデータ用回線インタフェースへ出力することにより、相手サービス事業者側の相互接続装置へパケットを送信して処理を終了する（ステップ２１２０、２１２５）。

【０１１４】図２２は相手のサービス事業者側からデータパケットを受信した相互接続装置における内部送信の処理動作を説明するフローチャートであり、以下、これについて説明する。この処理は、この処理は、図７に示すシーケンス７１０、７２０により説明した相互接続装置１１０－Ａからのデータパケットを受信した相互接続装置１１０－Ｂが、境界ルータ１２０－Ｂにパケットを送信する処理である。

【０１１５】（１）相手サービス事業者側の相互接続装置からデータ用回線を通してＩＰデータパケットを受信した相互接続装置は、そのデータパケットを受信したデータ用回線のＩ／Ｆ識別子が変換テーブルにすでに登録されているか否かを検索し、検索の結果、そのＩ／Ｆ識別子が既に変換テーブルに登録されているか否かをチェックする（ステップ２２０５、２２１０）。

【０１１６】（２）ステップ２２１０のチェックで、もし変換テーブルに該当Ｉ／Ｆ識別子がなければ、そのパケットを破棄してここでの処理を終了する（ステップ２２３０）。

【０１１７】（３）また、ステップ２２１０のチェックで、変換テーブルに該当Ｉ／Ｆ識別子があった場合、その変換情報のフラグが「有効」か否かをチェックし、フラグが「有効」でなければ、前述と同様にパケットを破棄してここでの処理を終了する（ステップ２２１５、２２３０）。

【０１１８】（４）ステップ２２１５のチェックで、変換情報のフラグが有効であれば、その変換情報に含まれる自サービス事業者側ＶＰＮ－ＩＤを含む自サービス事業者内通信用ヘッダを受信したＩＰパケットに付加し、そのパケットを境界ルータ側の回線へ送信する（ステップ２２２０、２２２５）。

【０１１９】

【発明の効果】前述したように、本発明の実施形態によれば、相互接続装置を利用して異なるＶＰＮの方式を用いている２つのサービス事業者の間で、複数のＶＰＮを相互に接続することができる。そして、本発明の実施形

態による相互接続装置は、管理情報を交換することによって転送するＶＰＮの設定を行っているため、ネットワーク管理者の手間を軽減することができる。また、相互接続時の相互接続装置間の回線には、通常のＩＰパケットが流れることになるため、一方のサービス事業者が内部での複数ＶＰＮ運用を提供していない場合は、通常のＩＰネットワーク機器を接続することによって特定のＶＰＮ―ＩＤに限ってＩＰパケットを送受信することができる。これらの結果、本発明の実施形態によれば、複数のサービス事業者が互いのＶＰＮを効率良く相互接続することができる。

【０１２０】

【発明の効果】以上説明したように本発明によれば、異なるサービス事業者のＶＰＮ相互を効率的に接続することを可能にした相互接続装置及びこれを用いたネットワークシステムを提供することができる。

【図面の簡単な説明】

【図１】本発明の相互接続装置を用いてサービス事業者間のＶＰＮ相互接続を行うネットワークシステムの構成例を示すブロック図である。

【図２】本発明の一実施形態による相互接続装置のハードウェア構成を示すブロック図である。

【図３】本発明の一実施形態による相互接続装置のソフトウェア構成を説明する図である。

【図４】本発明の一実施形態による相互接続装置が使用する変換テーブルの構成を説明する図である。

【図５】相互接続装置相互間のＶＰＮ変換情報の登録シーケンスを示す図である。

【図６】相互接続装置相互間のＶＰＮ変換情報の削除シーケンスを示す図である。

【図７】相互接続装置相互間でのデータパケットの送受信シーケンスを示す図である。

【図８】ＶＰＮ変換情報を登録しようとしたサービス事業者側の相互接続装置が他方の相互接続装置へ送信する登録メッセージの形式を示す図である。

【図９】登録メッセージを受信した相互接続装置が登録メッセージを送信してきた相互接続装置へ返信する登録完了メッセージの形式を示す図である。

【図１０】ＶＰＮ変換情報を削除しようとしたサービス事業者側の相互接続装置が他方の相互接続装置へ送信する削除メッセージの形式を示す図である。

【図１１】メッセージを受け取った相互接続装置が相手の相互接続装置へ返答する受信確認（ＡＣＫ）メッセージの形式を示す図である。

【図１２】メッセージの受け取り時にエラーが発生した場合に相手の相互接続装置へ送信する異常通知（ＮＯＴＩＦＹ）メッセージの形式を示す図である。

【図１３】ＶＰＮ変換情報を登録しようとしたサービス事業者側の相互接続装置における変換情報仮登録の処理動作を説明するフローチャートである。

【図１４】ＶＰＮ変換情報を削除しようとしたサービス事業者側の相互接続装置における変換情報削除の処理動作を説明するフローチャートである。

【図１５】登録メッセージを受信した相互接続装置における変換情報仮登録の処理動作を説明するフローチャートである。

【図１６】削除メッセージを受信した相互接続装置における変換情報仮削除の処理動作を説明するフローチャートである。

【図１７】管理者の登録承認を受けた相互接続装置における変換情報登録完了の処理動作を説明するフローチャートである。

【図１８】管理者の削除承認を受けた相互接続装置における変換情報削除完了の処理動作を説明するフローチャートである。

【図１９】登録完了メッセージを受信した相互接続装置における変換情報登録完了の処理動作を説明するフローチャートである。

【図２０】ＡＣＫメッセージを受信した相互接続装置における各種の処理動作を説明するフローチャートである。

【図２１】自サービス事業者側からデータパケットを受信した相互接続装置がそのパケットを外部に送信する外部送信処理の動作を説明するフローチャートである。

【図２２】相手のサービス事業者側からデータパケットを受信した相互接続装置における内部送信の処理動作を説明するフローチャートである。

【符号の説明】

１００－Ａ、１００－Ｂ　サービス事業者ネットワーク
１１０－Ａ、１１０－Ｂ　相互接続装置
１２０－Ａ、１２０－Ｂ　境界ルータ
１３０　データ用回線
１４０　管理用回線
２００　ＣＰＵ(Central Processing Unit)
２１０　メモリ
２１３　オペレーティングシステム（ＯＳ）
２１５　制御ソフト
２２０　内部ネットワークコントローラ
２２５　外部ネットワークコントローラ
２３０　キーボードコントローラ
２３５　キーボード
２４０　シリアルコントローラ
２４５　マウス
２５０　ディスプレイコントローラ
２５５　ディスプレイモニタ
２６０　ディスクコントローラ
２６５　ディスク装置
３１０　入出力制御部
３２０　変換管理テーブル
３２５　変換テーブル

25

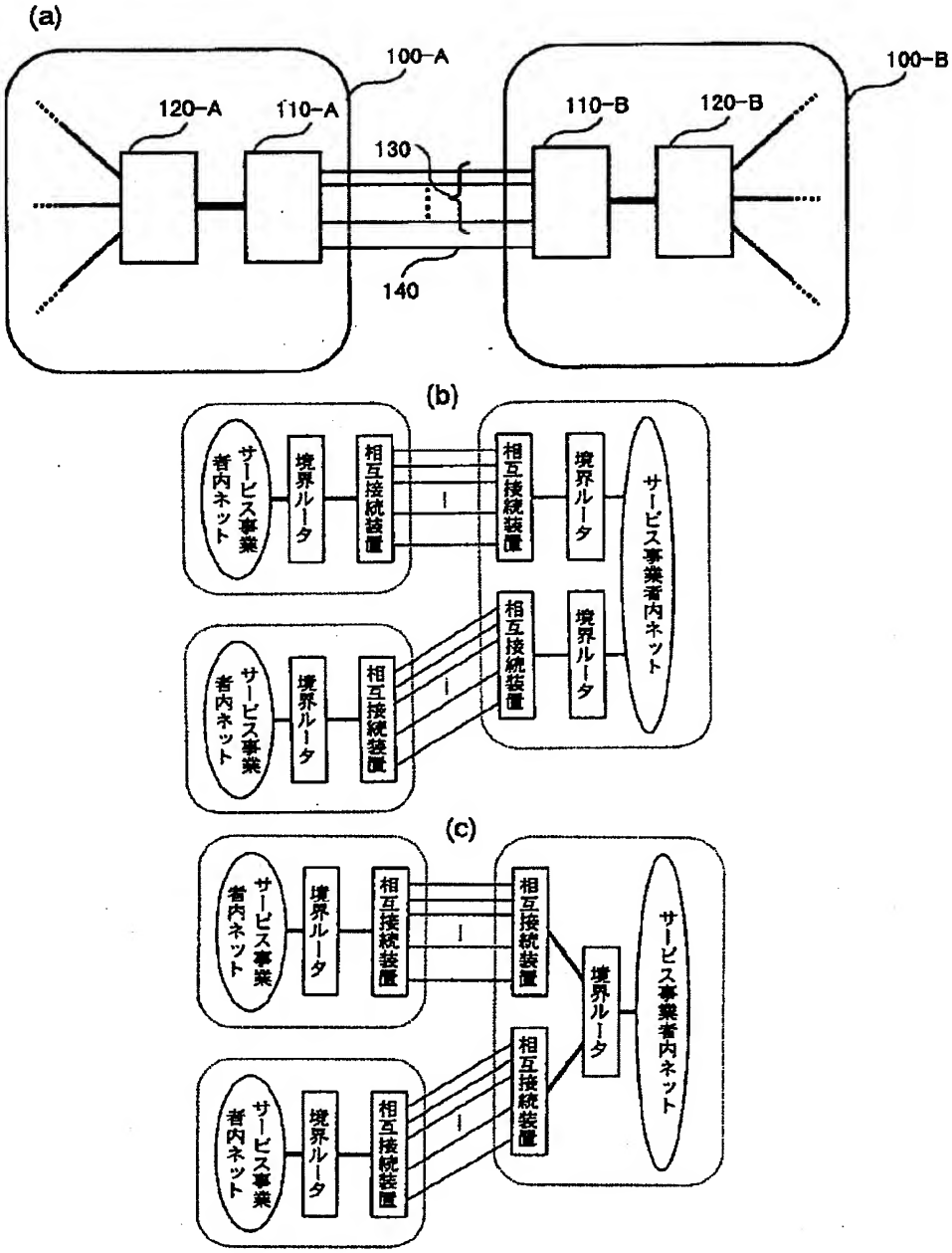
３３０　境界ルータ接続設定部
３４０　データ中継部
３５０　管理情報送受信部
３６０　境界ルータ通信部

26

３７０　外部回線通信部
３８０　内部ネットワークインタフェース部
３９０　外部ネットワークインタフェース部

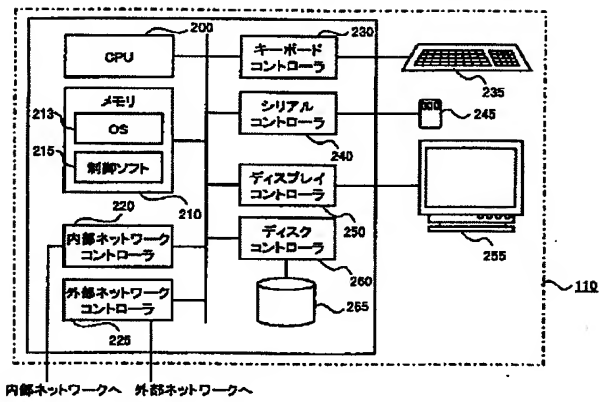
【図１】

図1



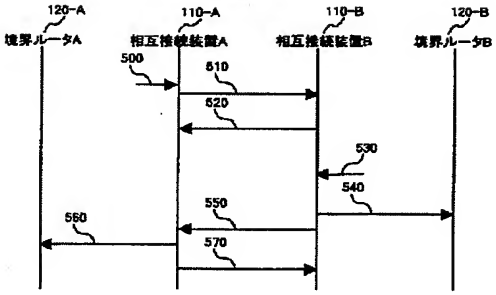
【図２】

図2



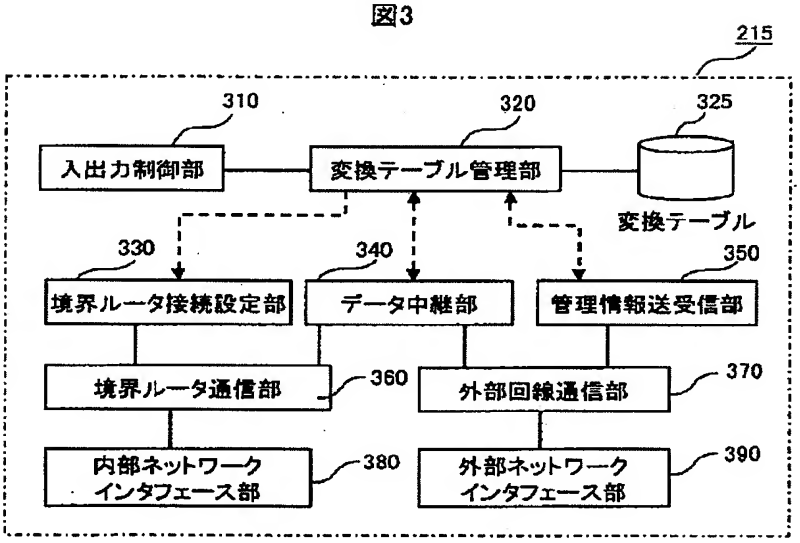
【図５】

図5



【図３】

図3



【図４】

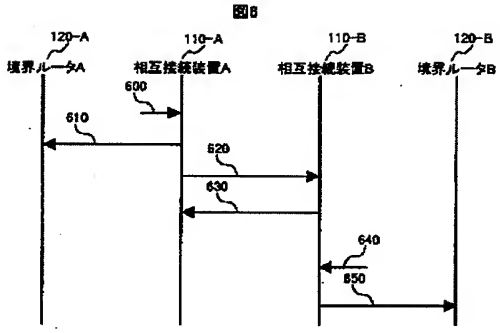
図4

325

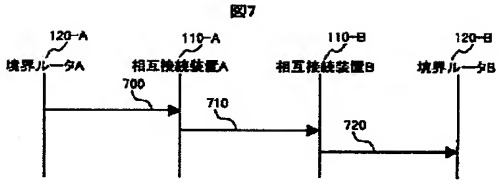
VPN-ID	相手VPN-ID	接続ネットマスク	ルータアドレス	相手ルータアドレス	I/F識別子	シーケンス番号	フラグ

410　420　430　440　450　460　470　480

【図６】

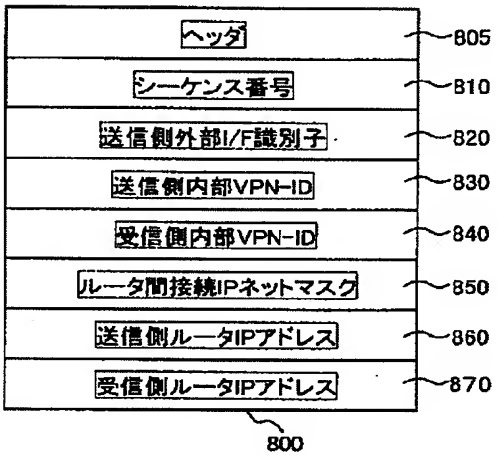


【図７】



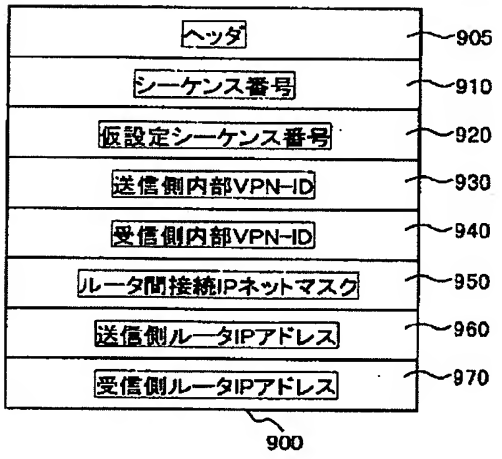
【図８】

図8



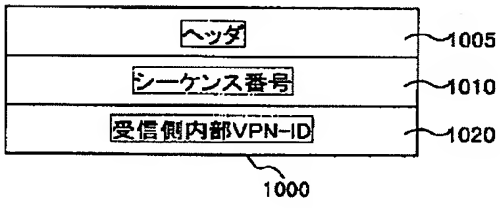
【図９】

図9



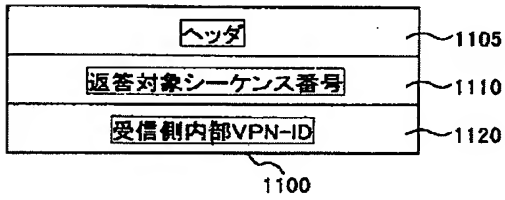
【図１０】

図10



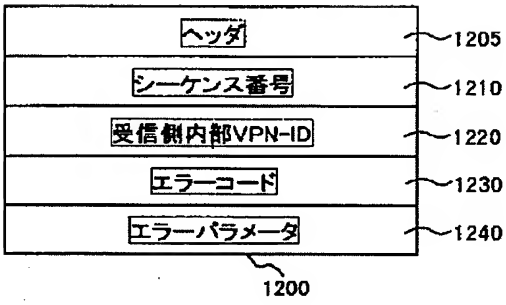
【図１１】

図11



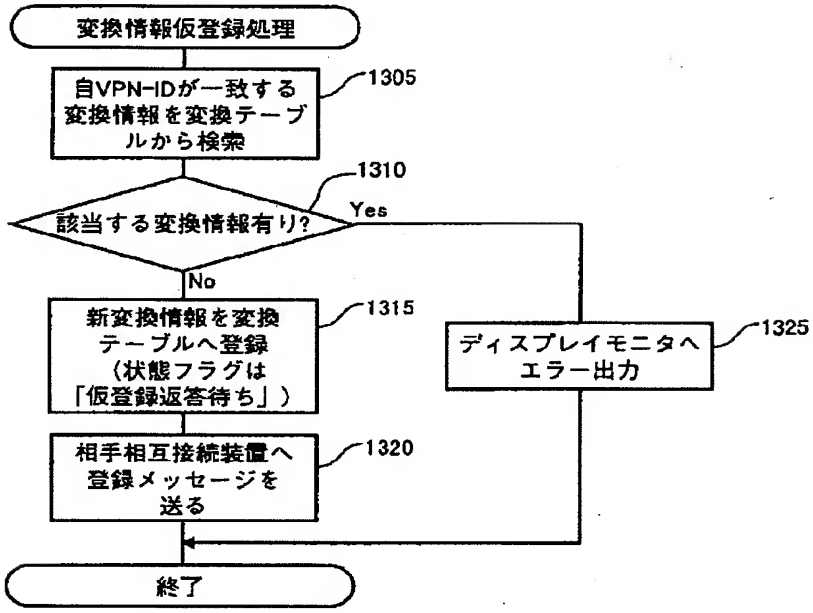
【図１２】

図12



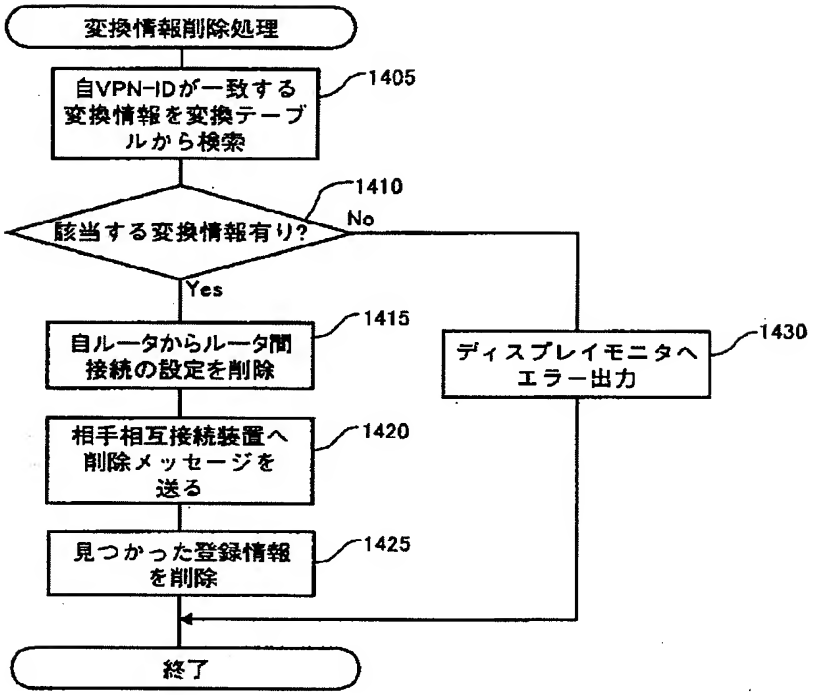
【図１３】

図13



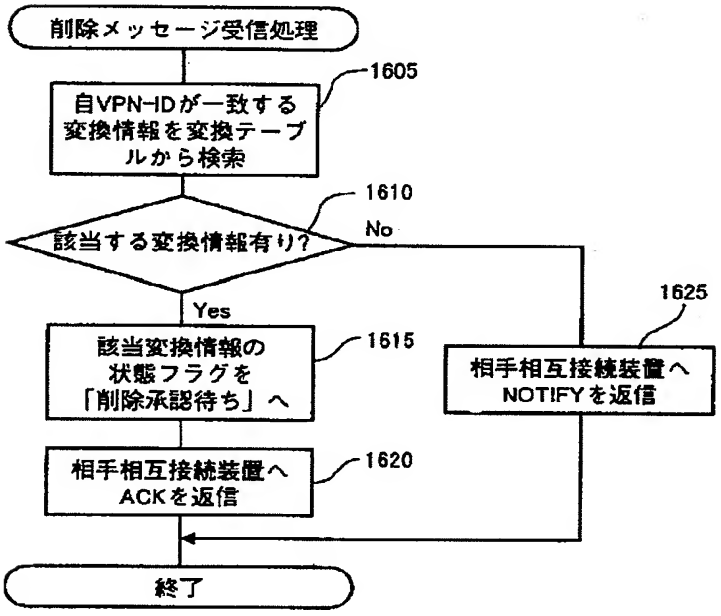
【図１４】

図14



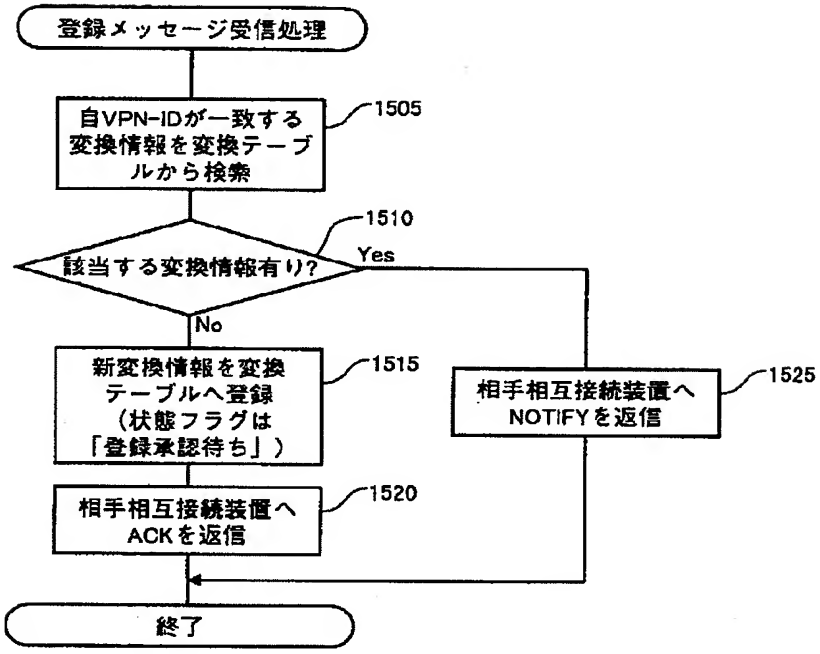
【図１６】

図16



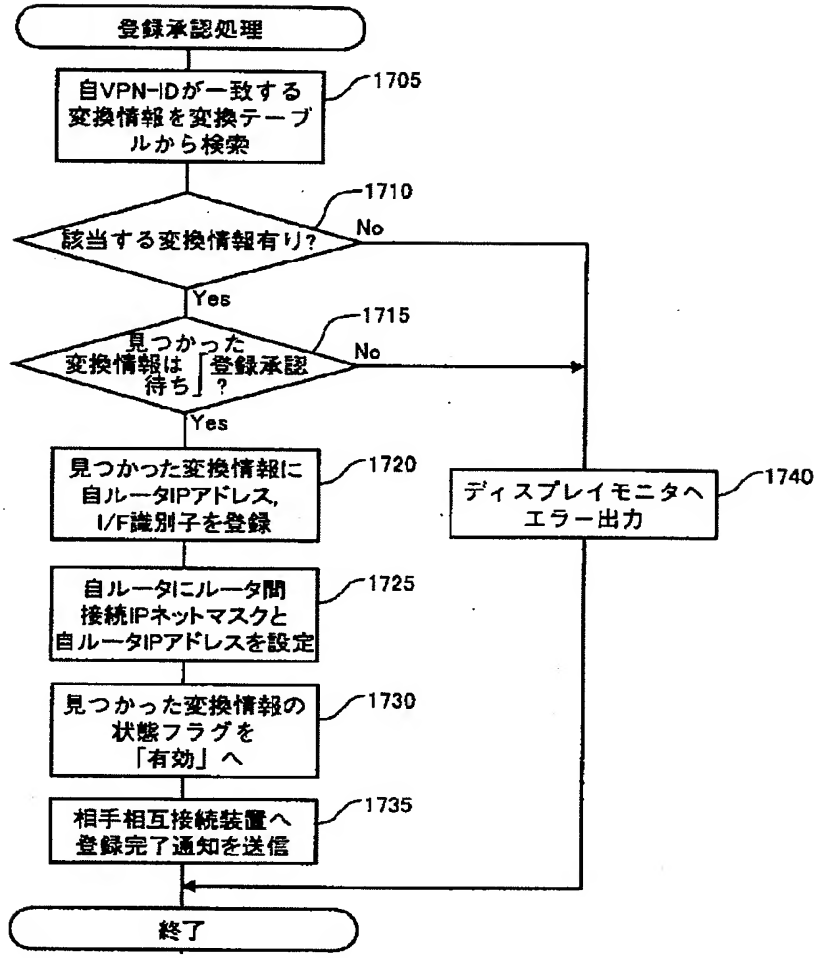
【図１５】

図15


登録メッセージ受信処理
自VPN-IDが一致する変換情報を変換テーブルから検索
1505
該当する変換情報有り?
1510
Yes
No
新変換情報を変換テーブルへ登録（状態フラグは「登録承認待ち」）
1515
相手相互接続装置へACKを返信
1520
相手相互接続装置へNOTIFYを返信
1525
終了

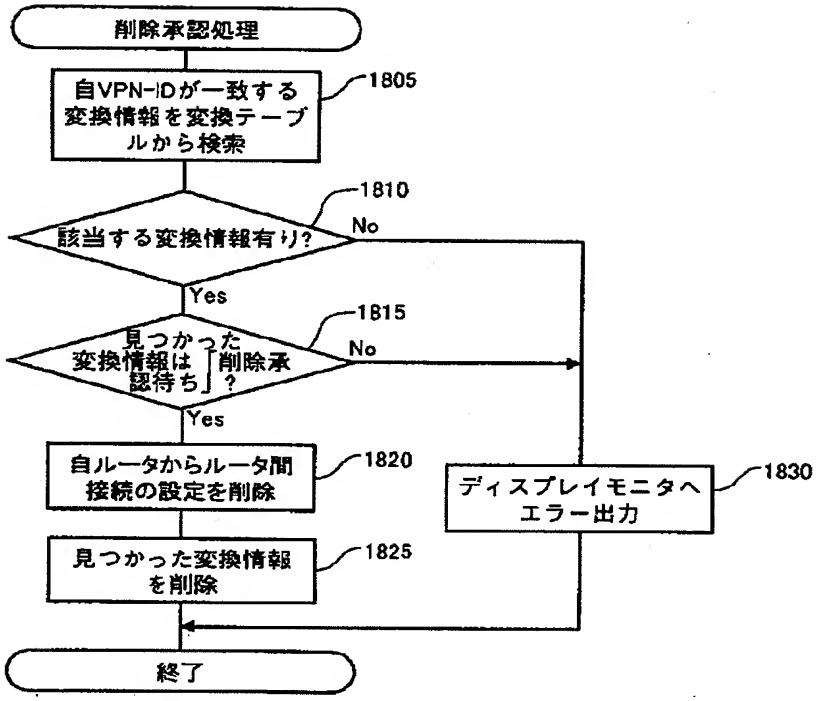
【図１７】

図17


登録承認処理
自VPN-IDが一致する変換情報を変換テーブルから検索
1705
該当する変換情報有り?
1710
No
Yes
見つかった変換情報は「登録承認待ち」?
1715
No
Yes
見つかった変換情報に自ルータIPアドレス, I/F識別子を登録
1720
自ルータにルータ間接続IPネットマスクと自ルータIPアドレスを設定
1725
見つかった変換情報の状態フラグを「有効」へ
1730
相手相互接続装置へ登録完了通知を送信
1735
ディスプレイモニタへエラー出力
1740
終了

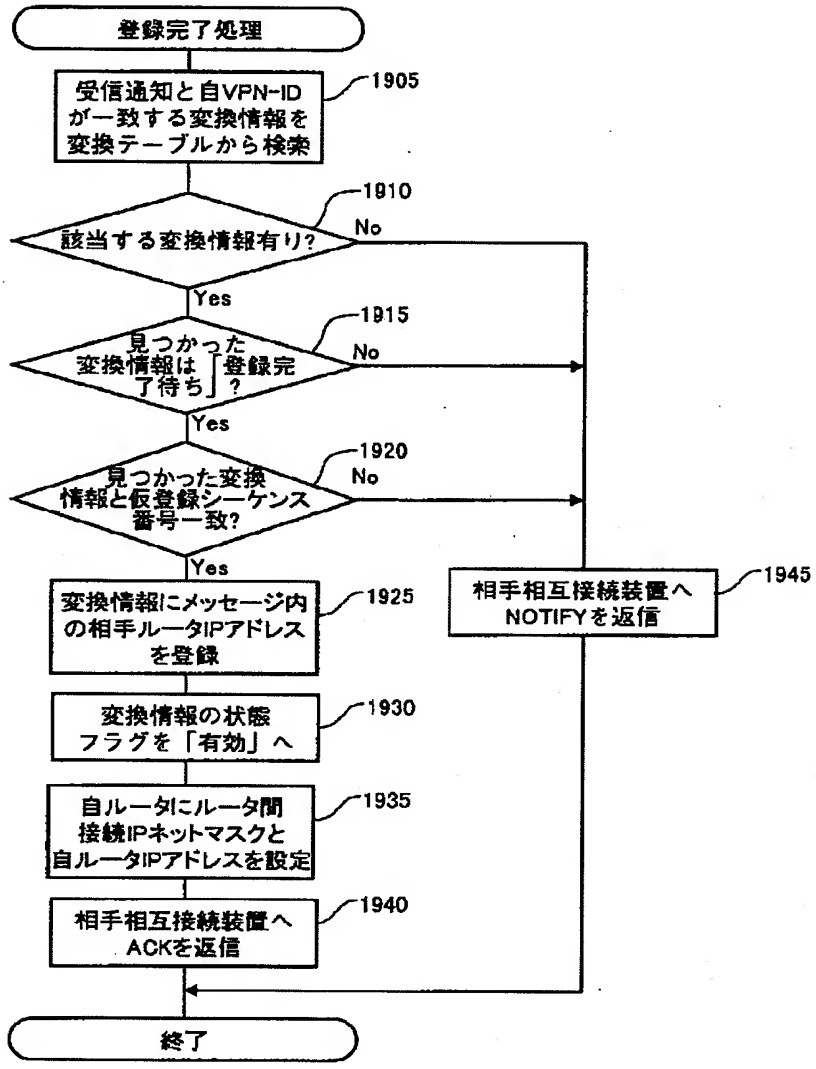
【図１８】

図18


削除承認処理
自VPN-IDが一致する変換情報を変換テーブルから検索
1805
該当する変換情報有り?
1810
No
Yes
見つかった変換情報は「削除承認待ち」?
1815
No
Yes
自ルータからルータ間接続の設定を削除
1820
見つかった変換情報を削除
1825
ディスプレイモニタへエラー出力
1830
終了

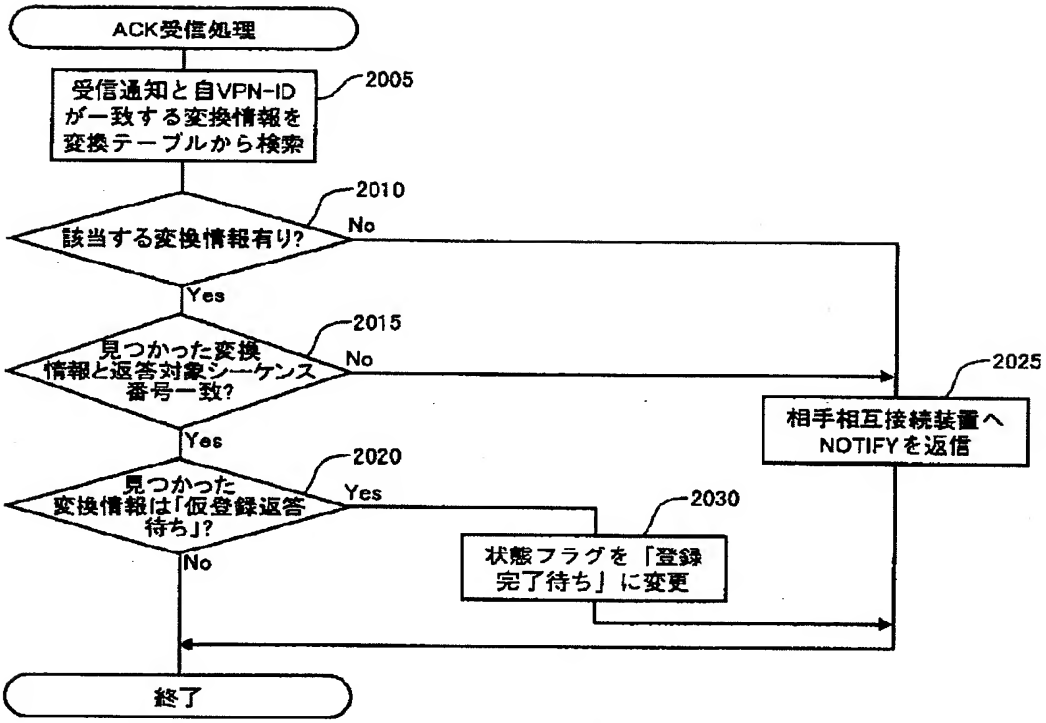
【図１９】

図19


登録完了処理
受信通知と自VPN-IDが一致する変換情報を変換テーブルから検索
1905
該当する変換情報有り?
1910
No
Yes
見つかった変換情報は「登録完了待ち」?
1915
No
Yes
見つかった変換情報と仮登録シーケンス番号一致?
1920
No
Yes
変換情報にメッセージ内の相手ルータIPアドレスを登録
1925
変換情報の状態フラグを「有効」へ
1930
自ルータにルータ間接続IPネットマスクと自ルータIPアドレスを設定
1935
相手相互接続装置へACKを返信
1940
相手相互接続装置へNOTIFYを返信
1945
終了

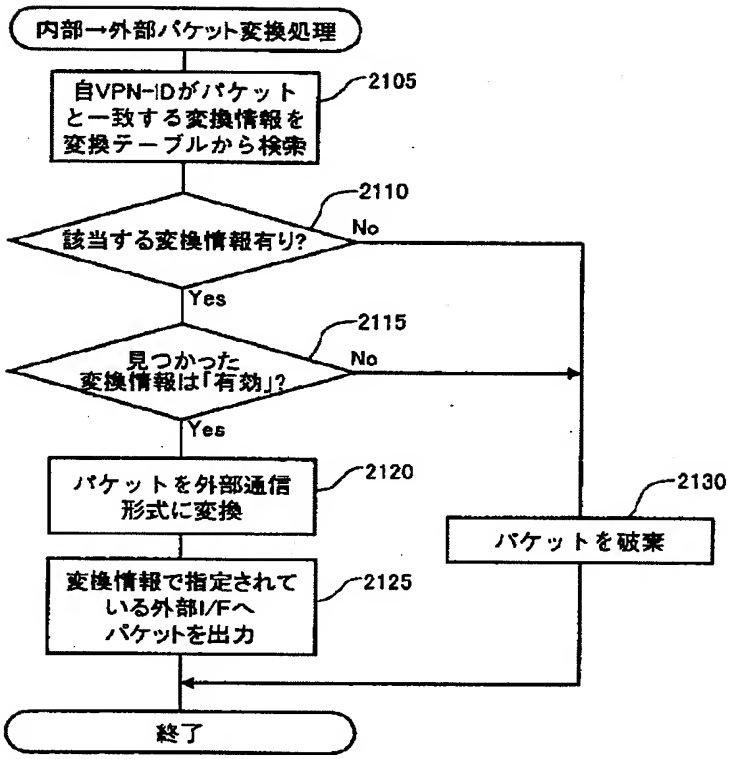
【図２０】

図20


ACK受信処理
受信通知と自VPN-IDが一致する変換情報を変換テーブルから検索
2005
該当する変換情報有り?
2010
No
Yes
見つかった変換情報と返答対象シーケンス番号一致?
2015
No
Yes
見つかった変換情報は「仮登録返答待ち」?
2020
Yes
No
状態フラグを「登録完了待ち」に変更
2030
相手相互接続装置へNOTIFYを返信
2025
終了

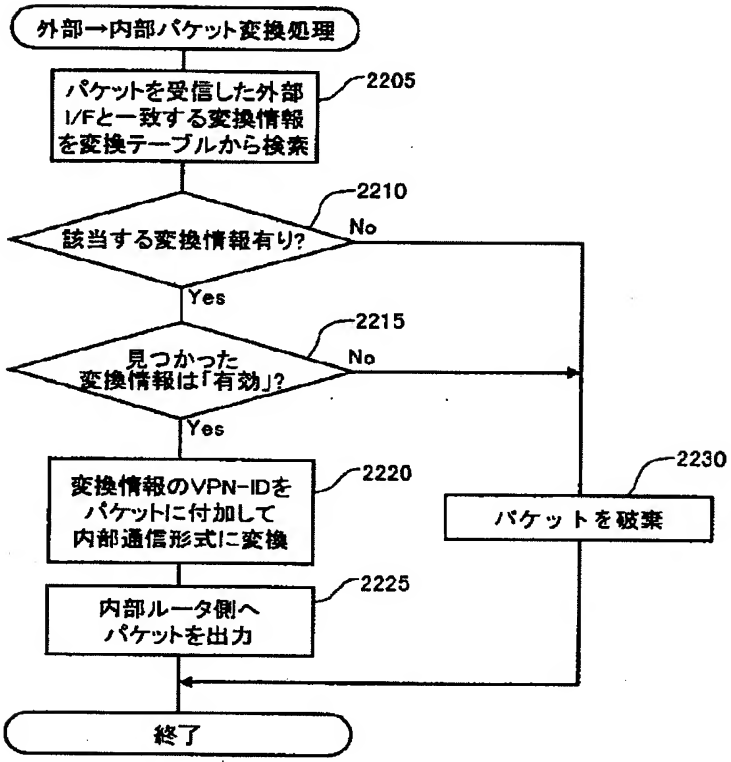
【図２１】

図21


内部→外部パケット変換処理
自VPN-IDがパケットと一致する変換情報を変換テーブルから検索
2105
該当する変換情報有り?
2110
No
Yes
見つかった変換情報は「有効」?
2115
No
Yes
パケットを外部通信形式に変換
2120
パケットを破棄
2130
変換情報で指定されている外部I/Fへパケットを出力
2125
終了

【図２２】

図22


外部→内部パケット変換処理
パケットを受信した外部I/Fと一致する変換情報を変換テーブルから検索
2205
該当する変換情報有り?
2210
No
Yes
見つかった変換情報は「有効」?
2215
No
Yes
変換情報のVPN-IDをパケットに付加して内部通信形式に変換
2220
パケットを破棄
2230
内部ルータ側へパケットを出力
2225
終了